EXCLUSIVE: Govt Documents Reveal DHS Domestic Spy Takeover

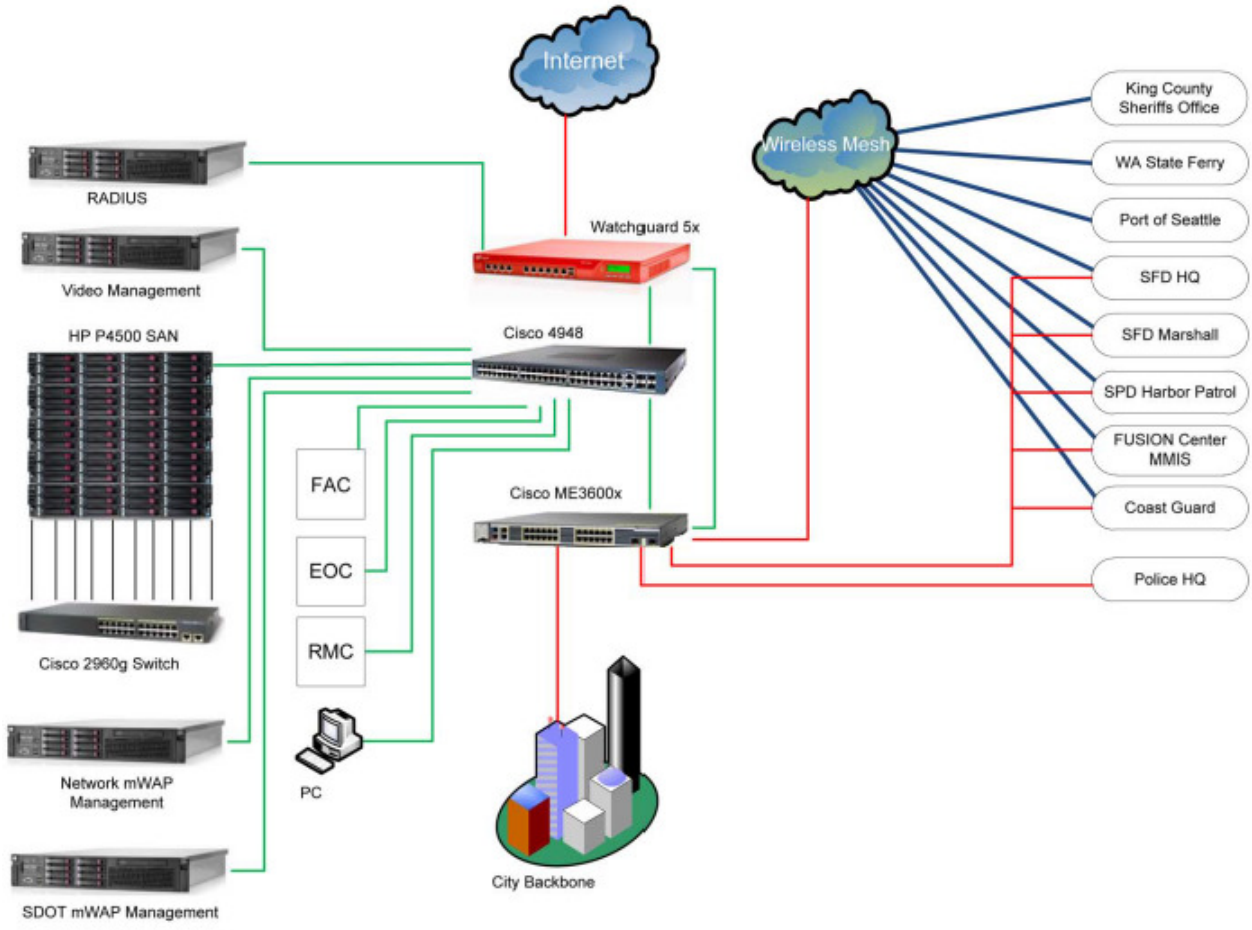
Posted By Anthony Gucciardi On November 12, 2013 @ 12:54 pm In Red Title Front Page,Tile | No Comments

Government documents obtained exclusively by Infowars expose massive DHS domestic spy grid designed to track citizens in real time through mega government databases.

Anthony Gucciardi & Mikael Thalen
Infowars.com
November 12, 2013

Exclusive documents obtained by Infowars from an insider government source have revealed the true origin and nature of the highly secretive 'mesh network' spy grid that has garnered massive media attention due to the fact that the network's strange downtown Seattle spy boxes can track the last 1,000 GPS locations of cellphone users. But as new documents reveal, the grid is far deeper than the media is telling you. The Seattle DHS spy system ultimately ties in with an enormous stealth database that acts as an intelligence hub for all of your personal data.

On page 55 of the "Port Security Video Surveillance System with Wireless Mesh Network" project document that we have obtained, a diagram reveals the system's basic communication abilities in regards to the Port of Seattle that the DHS has refused to comment on despite funding with millions in taxpayer dollars:



DHS spy system's basic communication abilities in regards to the Port of Seattle 'mesh network' tracking system.

The Infowars team is closely reviewing the document and will publish it in whole soon. More images

seen in the extensive documentation:


ONE WAY
MEXICAN KITCHEN
AUTHENTIC

A documented image of the actual spy system put in place, highlighted in the original document itself.

6.2.3 Project Organization and Personnel

Vendors must provide a Project organization chart identifying and showing the relationships between the Vendor, subcontractors, manufacturers and suppliers.

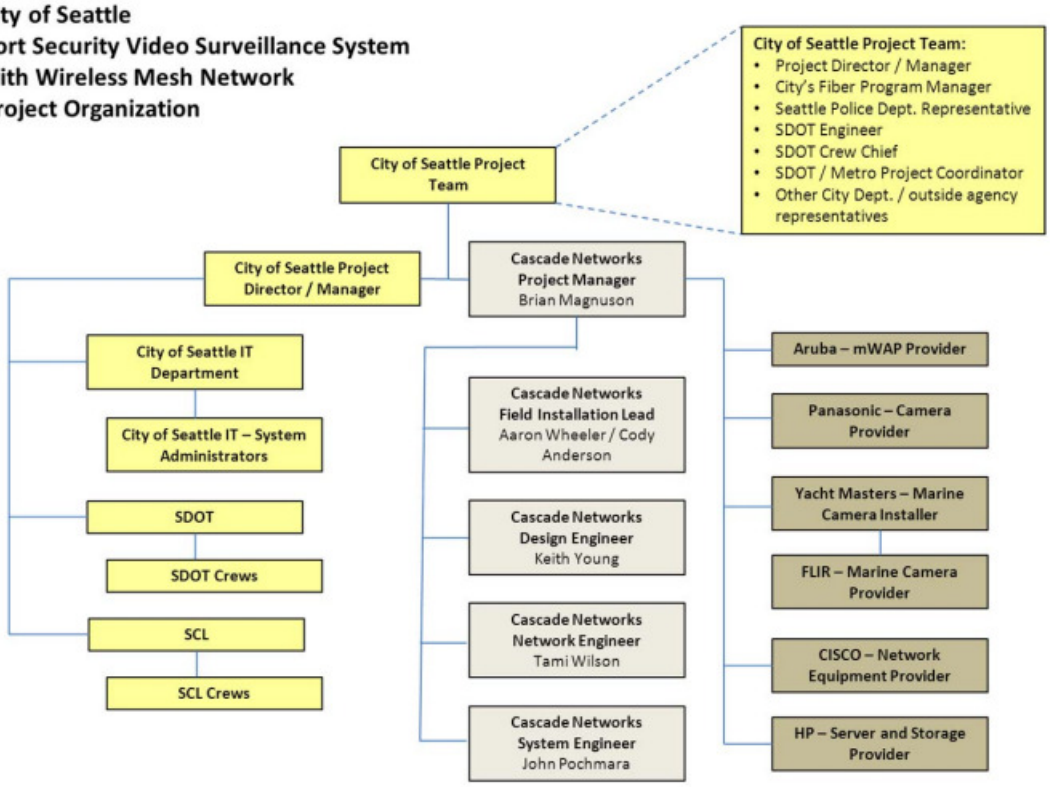
Key personnel to be assigned to the project by the Vendor and by any subcontractor, manufacturer or supplier should be identified and resumes provided.

Proposals must designate a project manager who will have overall, daily responsibility for the project. This person will be responsible for coordinating with the City project manager. Vendors must also designate a field wireless engineer/technician that will lead the combined City/Vendor field team in the installation of the system.

Proposals must include a resume of the Vendor's project manager and field engineer/technician. The City requires that the Vendor's field engineer/technician be available such that installation in coordination with SDOT (see Section 2.2 above), testing and integration services may be performed by the Vendor seven (7) days per week until December 15, 2012.

The City retains the right to reject proposed project personnel.

City of Seattle
Port Security Video Surveillance System
with Wireless Mesh Network
Project Organization



A further breakdown of the spy operation.

Download Video as MP4

The wireless mesh network, which allows for private communication between wireless devices including cell phones and laptops, was built by California-based Aruba Networks, a major provider of next-generation mobile network access solutions.

Labeled by their intersection location such as "1st&University" and "2nd& Seneca," the multiple network devices are easily detected in Seattle's downtown area through a simple Wi-Fi enabled device, leading many residents to wonder if they are being detected in return.

"How accurately can it geo-locate and track the movements of your phone, laptop, or any other wireless device by its MAC address? Can the network send that information to a database, allowing the SPD to reconstruct who was where at any given time, on any given day, without a warrant? Can the network see you now?" asked Seattle newspaper The Stranger.

According to reports from Kiro 7 News, the mesh network devices can capture a mobile user's IP address, mobile device type, apps used, current location and even historical location down to the last 1,000 places visited.

So far Seattle police have been tight-lipped about the network's roll-out, even denying that the system is operational. Several groups including the ACLU have submitted requests to learn the programs intended use, but days have turned to months as the mesh network continues its advancement.

According to The Stranger's investigation, Seattle Police detective Monty Moss claims the department has no plans to use the mesh network for surveillance… unless given approval by city council. Despite a recently passed ordinance requiring all potential surveillance equipment to be given city council approval and public review within 30 days of its implementation, the network has remained shrouded in secrecy.

Unknown to the public until now, information regarding the system has been hiding in plain view since last February at minimum. Diagrams attached to a March 2012 proposal request (# DIT-2996), which have since been approved, updated and finalized, are publicly viewable at the Seattle.gov website.

Several connections can be made by studying the diagram, including its now apparent link to Seattle's public waterfront. The recent instillation of 30 Department of Homeland Security-funded surveillance cameras on Seattle's popular waterfront, complete with mesh network devices attached, were purported to increase the Port of Seattle's protection against such acts as terrorism. Residents soon discovered multiple cameras facing inward toward Seattle homes, not towards the coast line as allegedly intended. The "accident" was later remedied by city officials.

While unknown members of multiple law enforcement agencies will have access to the mesh network, so will the Seattle Fusion Center, where FBI and Homeland Security gather data on Americans deemed "extremist" for such crimes as "loving liberty." Incredibly, even the U.S. Senate called the Fusion Centers a "useless and costly effort that tramples on civil liberties" in a 2012 bi-partisan report.

Page 65 of the public document details the information-collecting capabilities of the Mesh Network Mesh System (NMS), revealing its ability to collect identifying data of anyone "accessing the network." Although the document details an alert system for reporting unauthorized access, a public user guide from a similar Aruba software program lists the ability to collect "a wealth of information about unassociated devices," validating fears of local residents who walk through the mesh network's perimeter.

"The NMS also collects information about every Wi-Fi client accessing the network, including its MAC address, IP address, signal intensity, data rate and traffic status," the document reads. "Additional NMS features include a fault management system for issuing alarms and logging events according to a set of customizable filtering rules, along with centralized and version-controlled remote updating of the Aruba Mesh Operating System software."

The bottom left of the diagram shows what may be the Seattle Department of Transportation Intelligent Transportation Systems Network, linked directly into the mesh network. According to the Department of Transportation website, the system controls several surveillance related items such as license plate readers and closed circuit TV (CCTV) systems.

An early draft of the diagram appears to show Seattle police vehicle's ability to receive and "control" certain aspects of the mesh network. Whether police were originally intended to control surveillance cameras from their vehicles, including their panning, tilting and zooming abilities, remains unclear. According to statements made by Seattle's Assistant Chief Paul McDonagh last February regarding the waterfront cameras specifically, "only a few people would have that capability, so the officer on the street would just have the ability to view it."

In reality, Seattle is only one of countless cities across the country being flooded with a sea of surveillance equipment. While the public has focused mainly on surveillance issues relating to the NSA, the federal government has continued its 20-plus year dragnet surveillance grid roll out of covert conversation-recording microphones.

As recently reported by Storyleak, multiple cities including Las Vegas have begun using "Intellistreets" light fixtures capable of recording conversations. The device has received increased scrutiny since 2011 when their "Homeland Security" application, which shouts government messages from a loudspeaker system, was widely revealed to the public.

Other audio recording devices like the ShotSpotter microphones, allegedly used to analyze the location of gun shots, have been found to record conversations of unsuspecting city residents.

Despite the federal government's constant justification of throwing away civil liberties in the name of fighting terrorism, which kills less Americans than bee stings, continued NSA revelations show that the federal government's continued surveillance system build-up is aimed at everyday Americans, not foreign Al Qaeda admittedly supported by the U.S. government in Syria.

- Download
- Share
- Embed

of84

——-

Anthony Gucciardi is the acting Editor and Founder of alternative news website Storyleak.com. He is also a news media personality and analyst who has been featured on top news, radio, and television organizations including Drudge Report, Michael Savage's Savage Nation, Coast to Coast AM, and RT.

Mikael is an accomplished writer and lead features writer at Storyleak whose articles have been

featured on sites such as the Drudge Report and others. During his time at Examiner.com, he was frequently ranked the number one political writer.
